Amendments to the Specification

Replace the paragraph at pg. 3, line 31 which was amended by preliminary amendment to begin with "The figure depicts" with the following amended paragraph:

--Other characteristics, objects, and advantages of the invention will become apparent on reading the following detailed description, which is presented with reference to the appended figures, in which:

FIG. 1 is a schematic block ~~represents~~ representation of ~~The figure depicts~~ a certification infrastructure conforming to a preferred embodiment of the invention;

FIG. 2 is a flow chart illustrating the steps of a method in accordance with the invention; and

FIG. 3 is a block diagram illustrating the steps of the authentication performed in a step of the method of FIG. 2. --

On page 4, at line one, amend the paragraph beginning with "The idea is to" as follows:

-- Figure 1 is a schematic block representation of a certification infrastructure conforming to a preferred embodiment of the invention. With reference to figure 1, the ~~The~~ idea is to generate the key pair (public key + private key) in the user's mobile and then to forward the public key to a certification authority via a secure channel of the mobile telephone network.--

Insert at pg. 9, following line 28, the following paragraphs:

-- Figure 2 is a flow chart illustrating the steps of the method in accordance with the invention. The method uses a public key certification authority (30) and involves at least one mobile terminal (10) identified on a mobile telecommunications network, where the mobile terminal is configured to receive messages encrypted by a public certification key. With specific reference to FIG. 2, the method comprises generating, at the mobile terminal (10), the public certification key, as indicated in step 210. The public certification key is acquired at a telecommunications network entity (20) from the mobile terminal (10) via a network call located on the mobile telecommunications network, as indicated in step 220.

The mobile terminal (10) is authenticated at the telecommunications network entity by a party authentication process which is implemented in a standard telephone call on the mobile telecommunications network, as indicated in step 230. The public certification key and an associated authentication result are then supplied to the public key certification authority (30), as indicated in step 240.

Figure 3 is a flow chart illustrating steps of the method for authenticating the mobile terminal (10) in the method shown in Figure 2. Authenticating the mobile terminal includes sending, from the mobile terminal (10), a calculation result involving a confidential key stored in the mobile terminal, as indicated in step 310. The calculation result is compared, at the telecommunications network entity (20), with an expected result also calculated by the telecommunications

network entity (20) based on the same confidential key, a positive comparison result being an identification of the mobile terminal, as indicated in step 320. --